संख्या 110 /XXXIV/2004

प्रेषक:

एम0 रामचन्द्रन,
अपर मुख्य सचिव,
उत्तरांचल शासन।

सेवा में,

1. समस्त प्रमुख सचिव / सचिव,
2. समस्त विभागाध्यक्ष / कार्यालयाध्यक्ष
3. मण्डलायुक्त, गढ़वाल / कुमायूं।
4. कुलपति गढ़वाल विश्वविद्यालय, श्रीनगर / कुमायूं विश्वविद्यालय, नैनीताल / कृषि एवं प्रौद्योगिकी विश्वविद्यालय, पन्तनगर।
5. समस्त जिलाधिकारी, उत्तरांचल।
6. समन्वयक, एन0आई0सी0, उत्तरांचल सचिवालय परिसर, देहरादून।

सूचना प्रौद्योगिकी विभाग देहरादून: दिनांक: 7 अक्टूबर,2004

विषय: उत्तरांचल मे ई–गवर्नेन्स मानक का निर्धारण।

महोदय,

उपर्युक्त विषयक शासन द्वारा सम्यक विचारोपरान्त यह निर्णय लिया गया है कि सूचना प्रौद्योगिकी विभाग द्वारा "Standards for Application Architecture", "Standards for Content Management", "Standards for Web Designing" तथा "Standards for Security" आदि के मानकों का निर्धारण संलग्न विवरण में उल्लिखित शर्तानुसार किया गया है।

ई–गवर्नेन्स मानको का निर्धारण इसलिए आवश्यक है क्योंकि इससे–

1. गुणवत्ता, कार्यक्षमता, विश्वसनीयता तथा interchangeability कम व्यय पर उपलब्ध होती है।
2. विभिन्न अनुप्रयोगों का एक दूसरे के साथ डाटा एवं functionalities का आदान प्रदान सम्भव हो पाता है।
3. यदि सभी अनुप्रयोग एक ही मानक को आधार मानते हुए बनाए जाएगे तो उनमें integration, interactivity तथा reusability सम्भव हो पायेगी।
4. विभिन्न अनुप्रयोगों को विकसित करने के लिए होने वाला कुल व्यय कम से कम होगा।
5. विभिन्न प्रयोगों के बीच communication gap कम होगा।

अत: सभी विभागों से अपेक्षा की जाती है कि किसी भी तरह की Application Development/Content Management Activity/Web Designing Activity आदि के लिए

उपरोक्त मानकों का अनुपालन सुनिश्चित किया जायेगा ताकि Backend Integration/Interactivity, Security आदि सुनिश्चित की जा सकें।

उपरोक्त मानक मुख्यतः Open Plate Form/Linux के लिए है तथा DOTNET के लिए मानक www.microsoft.com पर उपलब्ध है।

उपरोक्त मानकों से विचलन की समस्त जिम्मेदारी सम्बन्धित विभागाध्यक्ष की होगी। यदि कोई विभाग उपरोक्त मानकों से उच्चतर मानकों पर कार्य करना चाहता है, तो कृपया उसकी सूचना, सूचना प्रौद्योगिकी विभाग, उत्तरांचल शासन को उपलब्ध कराने का कष्ट करें।

संलग्नक– यथोपरि।

भवदीय

(एम0 रामचन्द्रन)
अपर मुख्य सचिव

संख्या 110 (1)/XXXIV/2004, तद्‌दिनांक।

प्रतिलिपि– निम्नलिखित को आवश्यक कार्यवाही हेतु प्रेषितः–

1. विशेष कार्याधिकारी, मा0 मुख्यमंत्री, उत्तरांचल।
2. सचिवालय के समस्त अनुभाग।
3. गार्ड फाइल।

आज्ञा से

1/10

(अमरेन्द्र सिन्हा)
सचिव

Enclosure of G.O No. 110/XXXIV/2004 dated 7th October 2004 of
Department of Information Technology

Standards for eGovernment Applications Uttaranchal Portal

Version 1.0

(October 2004)

TABLE OF CONTENTS

1. Introduction

The Uttaranchal Portal aims to accomplish following.

- Support government objective to make available high quality services to citizens with a special focus on the poor.
- Help improve efficiency of government departments by providing means for better communication and reliable information.
- To provide information on Uttaranchal to other interested parties like businesses, investors and tourists.

The Uttaranchal Portal will provide information about the various government services, schemes and procedures through static and dynamic applications.

A Three-tier architecture consisting of front-end for citizen access, middle tier for transaction management, authentication, data protection, high-level security and back-end for providing connectivity to government departments and database, will be used for this portal. It is envisaged that the portal will be accessed by variety of people from various locations through different modes of access i.e. Internet, mobile devices, telephones etc. It shall be able to provide 24X7 days a week service. Portal will be PKI enabled and will be interfaced with mobile devices and smart cards. It shall have capability of upgradation vertically & horizontally. For Citizen-to-Government interaction through portal, the main paradigm would be HTML forms which are to be converted by the e-public service portal to XML and XSL-based interactions for e-filling, e-lookup, exception management etc.

The Static HTML pages shall provide the useful information from various departments of the state like objectives of a department, details of schemes/services offered by departments, current vacancies in a department etc.

2. Scope of the Document

This document intends to provide guidelines to various government departments for selecting technology for eGovernance initiatives to ensure, that applications, which would be developed in future, are able to interoperate and are flexible and portable enough to incorporate future requirements of the department without huge cost implications.

We recognise the pace at which technology is changing. This version represents best perspective for currently available technologies. However this standard must be reviewed and updated at least every six months to ensure that it incorporates latest technologies and trends.

These standards are meant to be guidelines for selecting suitable technology in accordance with business needs and available resources. These standards should necessarily not be considered as endorsement of a particular technology or product.

Scope of this document is as follows.

- Standards for Application Architecture
  - System Modelling (Data and Process Modelling)
  - Client Software
  - Presentation Tier
  - Middle Ware
  - Database
  - Backend Integration
  - Communication

- Standards for Content Management
    - Content Management (Processes Involved, Discovery of non-web content, Legal Requirements, Equity of access and maximum usability, Quality and functionality)
    - Content Accessibility (Publishing Formats, End User Browser Capability, Screen Resolution, Printability)
    - Discoverability
    - Information Management (Record keeping and disposal, Protection from unauthorized change, Publication status, Use of copyright information, Privacy)
- Standards for Web Designing
    - Web Page Design Guidelines
    - Home Page Design
    - Page Layout Design
    - Navigation
    - Scrolling and Paging
    - Heading, Titles and Labels
    - Hyperlinks
    - Text
- Standards for Security
    - Application Security Goals
    - Application Security Policy
    - Database Standards
    - Firewall Standards
    - Physical Security Standards
    - Anti Virus Software Requirements at the Client PCs

This document does not cover standards for following as a separate evaluation exercise was conducted prior to portal application development to evaluate hardware, operating systems and networking equipments.

- Hardware Standards
- Operating Systems Standards
- Networking Standards

3. Why Standards?

Standards are means to share ideas and to establish a common understanding on a given subject for all stakeholders, which eventually helps in minimizing communication gaps and building low cost solutions. By following standards one can ensure quality, efficiency, reliability and interchangeability at economical cost. The standards framework provides structure that one can follow and which helps everyone be on same page because they can see what is expected. It becomes easier for auditors, especially third party auditors, to effectively assess control against at least one base standard and then make recommendations over and above the standards, where appropriate. In Uttaranchal following are the driving forces for standards.

- To ensure that government services are available to every citizen of state irrespective of her/his level of literacy, disability etc.

- To ensure interoperability of various system/application being developed under eGovernment initiative.
- To ensure maximum utilization of existing investment in computational resources e.g. training, hardware and software.
- To ensure that solutions are flexible and portable enough to incorporate future requirements of the state without huge cost implications.

4. Methodology Adopted

Methodology chosen for developing standards for Uttaranchal is adoption of best practices from international standards. For this first international standards were reviewed and then selectively best practices or practices that are relevant to the Uttaranchal State were chosen,

To develop these standards following international standards were referred.

- COBIT (http://www.isaca.org/cobit.htm)
- ISO17799 (http://www.iso-17799.com/)
- ITIL (http://www.itil-itsm-world.com/)
- Technical Reference Model Version 1.1 of FEAPMO (Federal Enterprise Architecture Program Management Office)

Apart from these international standards, following specific standard implementations were also referred.

- SAGA-Standards and Architecture for eGovernment Application (http://www.kbst.bund.de/Anlage304420/Saga_2_0_en_final.pdf)
- Usability Guidelines from UsabilityGov, USA, BS7799 (ISO 17799) (http://usability.gov/pdfs/guidelines.html)
- Web publishing standards from Tasmania Gov (http://www.go.tas.gov.au/standards/tgwps/tgwps_complete_publication.shtml)

5. Architecture

The architecture, shown in following figure, outlines the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (Service Components) that may be used and leveraged in a Component-Based or Service Orientated Architecture.

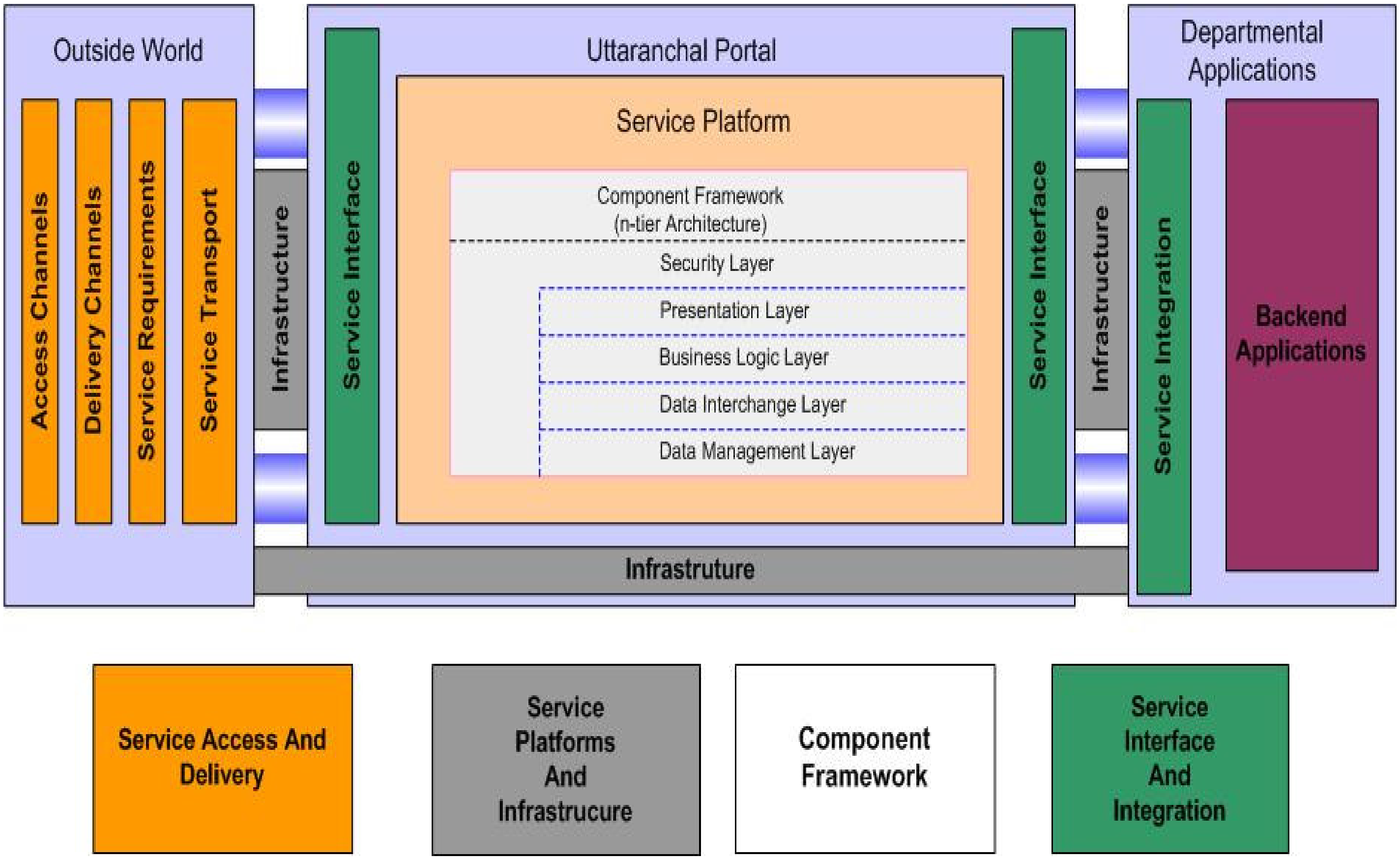


Figure 1. Architecture for Service Delivery

The architecture is comprised of four core Service Areas. Service Areas represent a technical tier supporting the secure construction, exchange, and delivery of Service Components. Each Service Area aggregates and groups the standards, specifications, and technologies into lower-level functional areas.

Service Access and Delivery refers to the collection of standards and specifications to support external access, exchange, and delivery of Service Components.

Service Platform & Infrastructure refers to the collection of delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component.

Component Framework refers to the underlying foundation, technologies, standards, and specifications by which Service Components are built, exchanged, and deployed across Component-Based, Distributed, or Service-Orientated Architectures.

Service Interface and Integration refers to the collection of technologies, methodologies, standards, and specifications that govern how various departments will interface (both internally and externally) with a Service Component. This area also defines the methods by which components will interface and integrate with back office applications.

Each service area consists of multiple service categories, service standards and service specification. This document presents standards for various service categories shown in above diagram e.g. Access Channels, delivery channels, service requirement service transport etc.

6. Classification of Standards

Standards are classified in three categories namely mandatory, recommended and emerging.

Mandatory: Standards which are tried and tested and represent preferred solution.

Recommended: Standards which are tried and tested, but are not mandatory and/or do not represent the preferred solution.

Emerging: Standards which are in line with the intended development trend, but they have not achieved a mature level.

Under Evaluation: Standards which are being considered for incorporation.

7. Standards for Application Architecture

7.1 System Modelling (Data and Process Modelling)

In a software system apart from an executable there are other artifacts that complement the executable. Examples of these artifacts are requirement document, design documents and testing documents. There are various techniques to document requirements and design of a system e.g. ERD, DFD, data modeling, UML etc. In Object Oriented Programming regime process modeling and data modeling techniques are the stories of bygone days. Latest paradigm for modeling a system's behavior is UML that keeps both data and processes together. Also UML notations are standard which is not true in the case of ERD or DFD. It is recommended to use UML as modeling for unified modeling of data and behavior rather that using DFD, Flow Charts, ERD to model processes and behavior separately. Following is the list of artifacts that must be prepared for modeling a software system. (* indicates mandatory artifact).

Mandatory: UML Following standards are applicable for object oriented modeling	
Requirements Analysis	Use Cases * and Use Case Diagram *
For Modeling Entities and Their Behavior	Class Diagram *
	Class Relationship Diagram *
For Modeling Process Flow	Activity Diagram
	Collaboration Diagram *
	Sequence Diagram *
State Transitions	State Chart Diagram

Recommended: ERD, DFD and Flowcharts Following standards are applicable for data centric modeling	
Requirements Analysis	Simple Text
For Modeling Entities	Entity Diagrams
	Entity Relationship Diagram
For Modeling Process Flow	Data Flow Diagram
	Flow Charts

7.2 Application Architecture

Application architecture framework must be based on open standards and must offer portability across different platforms.

3-Tier Architecture	**Mandatory-**J2EE Framework
	Emerging-.NET Framework

3-Tier architecture has following layers.

- Presentation Layer
- Middleware
- Database

7.2.1 Access Channels

Client software is a group of products that are used by users of an application to access the services offered.

Web Based

Web based clients are the browsers that enable access to internet based services. Web base access ensure wide spread use of the eGovernment applications.

Browser Capabilities	Selected browser must support JavaScript 1.3, CSS Level 2, HTML 4.01, Flash 7.0, XML 1.0
Monitor Size and Resolution	Minimum 15 inches monitor with 800 X 600 resolution and minimum color quality of 24 bit.
Screen Resolution	800 X 600
Presentation-Client	HTML 4.01, Stylesheets. Any formatting information must not be embedded in HTML code.
Scripting-Client	JavaScript 1.3. It must comply with ECMA-262.
Cookies	At browser use of cookies should be avoided and any private information should not be cached for performance reasons. One must not store sensitive information like passwords, credit card numbers etc. in cookies. After user leaves the site all cookies must be deleted to ensure that no body is able to tamper cookies. This control is implemented at application level.
Usage of Active-X	Prohibited for security reasons as an Active-X has unlimited access to the resources of a system on which it is running.
Applets	Applets can be used only if it is absolutely necessary and other implementation alternatives are not possible. Applet does not pose security threats as applets run in a controlled environment and does not have unlimited access to the resources of a system on which it is running. However each applet that is used must be signed by the server so that user is sure about the source.
Browser Configuration	Configuration Examples are prepared for usual browser types and made publicly available on the internet. These examples must contain browser setting for enhanced performance of application, security setting etc.
Communication Protocol	HTTP (V1.1), HTTPS
Plug-ins	A list of supported and required plug-ins must be published at portal web-site.

E-Mail Client

SMTP	For receiving and ending E-Mails.
MIME	As the e-mail format description.
Access Mode	E-Mail solution must allow accessing emails from web browser as well as from thick email clients.

Access via Mobile Phone

Access via mobile phones is a convenient means to access limited application services.

SMS	Preference must be given to SMS due to its wide acceptability in users. Short Message Services are to be implemented on the basis of the specifications issued by the SMS Forum[1]. The SMS Forum is an international forum of all major IT companies.
WML	The Wireless Application Protocol (WAP) v1.x is a specification for the development of applications that use wireless communication networks. Its main application is mobile communications. It requires WML browser to be installed on a mobile device.
J2ME	This can be used for building java based mobile application for mobile devices. For this mobile device should be java enabled (MIDP 1.0). Though mobiles devices with MIDP 2.0 are available, but to have backward compatibility application must conform to specification MIDP 1.0.

Access from Client Applications

Client application can be used where functionality of web-browser is not adequate to support a business function e.g. accessing file system for a business transaction. These applications are installed on the client and must be updated as and when required.

Architecture	3-Tier
Language	Java as it is platform independent. (Mandatory) .NET Platform (Emerging)
Local Storage	Any critical/sensitive information must be stored in encrypted form.
Access Mechanism	Web Services for both non J2EE and J2EE clients.
Communication Protocol	HTTP 4.01, HTTPS, SOAP V1.1
Information Interchange	XML
Accessibility to Disabled	See section 5.2.2→ Presentation for disabled
Updates	Software updates to the client software can be provided in following formats. 1. CD-ROM 2. Downloadable from Web Site.

7.2.2 Presentation

The presentation element provides the client tier with information. Depending on the given application, different formats must be made available. These are listed in the following sections. The use of open interchange formats which offer a sufficient number of functions and which are available on different platforms is generally required. Following table lists the standards to be used for information processing.

Character Set	UTF-8 for Hindi display. (Mandatory)
Presentation for the disabled	All pages of all web sites must be at least Priority 1 compliant with W3C Web Content Accessibility Guidelines 1.0. Available at:

[1] http://www.smsforum.net/

	http://www.w3.org/tr/wai-webcontent
	Disabled person (blind or visually impaired persons) should be able to access the documents in a form perceptible for them e.g. in oral form. **Mandatory**-Screen readers (in Hindi). **Recommended**-Prerecorded audio can be used but it is a costly implementation as it involves huge storage and maintenance cost.
Interchange format for Hypertext	**Mandatory-**HTML 4.01
	Emerging-XHTML V 1.0- This is still a W3C recommendation and it will be fully supported in future generation of browsers.
Presentation-Server (Static Content)	**Mandatory-** HTML V 4.01
	1. HTML V 4.01 must be used for static content. 2. XML along with XSL and XSLT may be for generating HTML pages. This helps in keeping content and presentation separately. However due to lack of XQuery engines this technology should be observed for some time.
Presentation-Server (Dynamic Content)	**Mandatory-**JSP 1.2, Servlets 2.3, XML V1.0, XSL **Emerging-**ASP.NET
	1. JSP is able to generate to HTML and XML dynamically. 2. It must not have direct calls to database through JDBC for ensuring flexibility and reusability of application components. It must request business components for getting data from database. 3. Scriptlets should not be used for generating dynamic HTML pages. Recommended technology to use is tag libraries. 4. One must use resource bundles for displaying static text/labels to ensure multilingual support at presentation layer. 5. Wherever possible instead of building HTML pages for static content, XML along with XSL and XSLT should be generating for HTML pages. This helps in keeping content and presentation. However due to lack of XQuery engines this technology should be observed for some time.
Style Sheets	**Mandatory-** Cascading Style Sheets Language Level 2 (CSS2)
File Formats for Document	**Mandatory-**.txt (Text) for documents that can be edited
	Mandatory- Portable Document format (.pdf) for documents that cannot be edited.
	Mandatory- Hypertext Markup Language (.html) for hypertext documents.
	Mandatory- The MIME format must be used for the standardized definition of the format of a file or any part thereof. It enables email client and web browser to identify the file type.
Interchange formats for Graphics	**Recommended**- PNG-It supports interlacing hence allows the browser to display portions of the image as it updates. It is faster in loading. It is best used for typical logos, line-art drawing, animation, and screen captures. Its compression is lossless. However older browser does not support this. There is no licensing issue for using this format.
	Mandatory- JPEG is best suited for photographic quality images and it is not suited for line art.
	Mandatory- GIF-This can store maximum 256 colors. It supports interlacing hence allows the browser to display portions of the image as it updates. It is faster in loading. It is best used for typical logos, line-art, drawing, animation, and screen captures. This format should be used only if colors used in a picture are less than 257.
	Recommended- TIFF-should be used for graphic information that does

	not permit any loss of information.
	Recommended- Enhanced Compressed Wavelet (ECW)-It should be used whenever maximum compression is required.
Interchange formats for audio and video files	**Mandatory-** MPEG-1 Layer 3 (mp3) for audio. A plug-in is required in browser to play these files.
	Mandatory- There are various formats available from different vendors. Quciktime, AFS, MOV can be used for video file however a suitable plug-in is required in the browser to play these files.
	Emerging Ogg-It is a manufacturer independent compression format for audio (Vorbis) and video (Ogg Theora, Ogg Tarkin) and aims to replace proprietary audio and video formats. This technology should be used in future for streaming media.
Interchange formats for audio and video streaming	There are many technologies by different vendors (Microsoft, Apple, Real Networks etc.) in this area. This standard does not intend to give recommendation for any single product. However broad outlines for selection of a streaming media server are as follows. **Mandatory-** Transfer Protocol: RTP **Mandatory-** Control Protocol: RTSP **Mandatory-** Network Protocol: IP **Mandatory-** It should be noted that Http is not suitable for transferring media with timelines as it is based on TCP which enforces reliability without regard to timeliness.
Animations	**Mandatory-**Animated GIF
Data compression	**Mandatory-**Zip V 2.0
	Under Evaluation-GZIP 4.3
Information Processing – External Systems	See topic 5.2.5 Backend Integration

7.2.3 Middleware

This layer of an application offers services such as business logic, transactions management, messaging applications, internationalization, etc. to an application. This layer is very important as it is the foundation block for interoperability and portability.

Design Patterns	**Mandatory-**Struts (Implementation of Model, View, Controller Pattern)
	Mandatory-Hibernate for Persistence **Recommended**-EJB CMP
Persistence	**Mandatory-**Hibernate for Persistence **Recommended**-EJB CMP 1. In no case one should use proprietary classes of a J2EE application server provider for using extensions of CMP as these results in loss of portability. 2. BMP can be used when CMP or Hibernate is not able to deliver desired results/performance. However its usage should be avoided.

Security	**Mandatory-** JAAS V1.0- Authorization and Authentication are to be implemented using JAAS as it offers integration into authentication of Unix, Windows NT and Kerberos.
Messaging	**Mandatory-** JMS 1.0
	1. One is not allowed creating more than one session per active connection. 2. It must support point to point and publish subscribe messaging 3. An application component must not use following any interfaces that have implication on portability.
Database connectivity	**Mandatory-**JDBC 2.0 **Recommended**-ODBC
	1. It must able to connect variety of database to ensure portability. 2. One must be able to access database from web components (not recommended), EJB components and application client components. 3. Driver for database connectivity must meet JDBC compatibility requirements in JDBC specification. 4. One must use JNDI look for loading database drivers instead of loading database drivers directly.
Runtime Environment	**Mandatory-**JDK 1.4
Business Logic Components	**Mandatory-**Stateless session beans for modeling business processes. **Mandatory-**Web Services
	1. Business logic must be written in session beans. Entity beans should be used as a mean of data access only (If chosen persistence mechanism is entity beans). 2. It should be possible to transform output of a session bean method to XML and to expose a method as web service. 3. A stateless session bean must not access data directly from the database using JDBC. It must use Data Access Object framework (Entity beans, Hibernate, JDO) to access data. 4. Wherever there is need to exchange data with other organizations, method interfaces must be agreed upon by involved parties.
Naming Services	**Mandatory-**JNDI 1.2.1
	1. Applications must access resources and external information in their operational environment without knowledge of how the external information is named and organized in that environment. For this it becomes absolutely necessary to use naming services. 2. One must use naming services for EJB lookup, getting JDBC and JMS connection etc.
Web server extension/Controller	**Mandatory-**Servlet 2.3
	1. Servlets provide extension to web-server's capabilities. Though servlets are able to generate presentations, it must be used only to control the application flow. 2. Servlets must not be used to generate presentation. 3. All objects that needs to be moved across virtual machines (for distributed applications), must implement java.io.serializable interface. 4. Local access to enterprise beans must not be made from servlets in order to ensure scalability and clustering of web servers. 5. It must not have direct calls to database through JDBC for ensuring flexibility and reusability of application components. It must request EJB components for data needs.

Administration, Data Definition and System Parameters	**Mandatory-**XML
Directory Services	**Mandatory-**LDAP V3
Bilingual Support	**Mandatory-**Using Unicode and resource bundles (for static text on screen).
Transaction Management	
	Mandatory-One must use of container's transaction management service. **Mandatory-**Any application component should not attempt to control the transaction characteristics of JDBC connection, commit the transaction or rollback the transaction.
XML Query	**Emerging-**Xquery, To access a collection of XML files like database. Xquery is still in draft status.
XML Transformation	**Mandatory-**XSL to convert XML document in HTML. **Recommended**-JAXP (it results in tightly coupled parses with a XML schema).
Content Management	**Mandatory-**Content management software must have following features
	It must allow creating documents. It must have an integrated approval workflow It must allow versioning of document. It must allow archiving of the documents. It must support various document formats like .doc, .pdf etc.

7.2.4 Database

Database provides storage for persistent data.

Type	Relational
Standard	Any ANSI SQL 92 Complaint e.g. Oracle, DB2 or SQL Server

7.2.5 Backend Integration

There are two aspects of information interchange one is technical feasibility and other standardization of interfaces for data interchange among various organizations. Technical feasibility is ensured by following standards for interoperability e.g. Web Services, XML, XSLT and standardization of character sets being used. Standardization of interfaces for data interchange will be done at state level, to ensure that need of all the organizations for sharing data are met. Technically to enable interoperability following standards must be followed.

Character Set	**Mandatory-**Unicode, for Hindi charset UTF-8 is to be used. One must remember that these are double byte code sets hence appropriate care must be taken while defining the data lengths as most database support defining data length in bytes not in number of characters. Also any software that processes information during data interchange must be capable of handling these character sets.
Data Exposure/Format	**Mandatory-**Web Services and XML formats. In no case any other format like csv, spreadsheet etc. should be used for information interchange.
	Mandatory-XSD V1.0 for defining XML schemas for data interchange.
Data Transformation	**Mandatory-**XSLT V 1.0 for declarative transformation **Recommended**-JAXP (Java API for XML Parsing) for programmatic transformation.
Integration with Legacy Systems	**Mandatory-**Standard business process integration tool e.g. Web Methods, IBM Business Process Choreographer etc. (preferred

	Methods, IBM Business Process Choreographer etc. (preferred approach but high cost) **Recommended**-J2CA 1.0 with JMS 1.0 for writing custom programs for integration (suitable for small to medium system integration problems, low cost).
Data Identification	**Mandatory-**Any system that intends to integrate with portal must be capable of identifying portion of data in their respective databases that is to be created or updated at portal.

Mechanism for Data Interchange with Backend Applications

Backend integration will be jointly done by portal team and backend application development team. Both development teams have to establish rules and contract through which data will be exchanged. This will involve defining XML schemas for information interchange, agreement on master information (e.g. code of organization to use), rules for data transformation etc.

FROM BACKEND APPLICATION TO PORTAL SERVER (PUSH)	Web Services will be used for exchanging data with back-end systems. Updation of data at portal server can be real time or periodic. It will be responsibility of backend system to push data to central server and it will be responsibility of central server to provide necessary programming interfaces using which data can be pushed to central server.
Synchronous	Data is updated instantaneously on central server. Web services will be standard for updating information real time on central server. This is not a recommended approach.
Asynchronous	A batch process runs which invokes web-services for data updation in central server. To implement this, a messaging solution is needed at departmental application end that is able to queue and manage the message requests and transfers data periodically to central server. One can use custom built message frameworks complying with messaging standards mentioned above or a standard messaging solution (MS-MQ, MQ-Series) for implementing this. Choice of implementation will depend upon availability of funds and messaging needs of an organization. Fundamentally this solution should be able to invoke web services running at central server for exchanging data. This approach eliminates need of any messaging solution at central server however it is very important that central server is up when batch processes are running.
FROM CENTRAL SERVER TO BACKEND APPLICATION (PULL)	It will be responsibility of backend system to pull data from central server and it will be responsibility of central server to provide necessary programming interfaces using which data can be pulled to from server. Then backend applications must have necessary software's that are able to read, interpret and load that data into backend application databases.
Synchronous	For this portal application must be able to send an alert to backend application whenever there is a change in data at central server. Then backend application will call appropriate Web service to pull data and load it in backend application database. It will require portal server to implement a messaging solution that is able to alert backend application for changes in data.

Asynchronous	A batch process runs, which invokes web-services to pull data in central server. To implement this, a messaging solution is needed at departmental application end that is able to queue and manage the message alerts and transfers data periodically from central server. One can use custom, built message frameworks complying with messaging standards mentioned above or a standard messaging solution (MS-MQ, MQ-Series) for implementing this. Choice of implementation will depend upon availability of funds and messaging needs of an organization. Fundamentally this solution should be able to invoke web services running at central server for exchanging data.

Following is the list of master databases that need to be prepared at state level.

- State
- Division
- District
- Sub-Division
- Tehsil
- Panchayat
- Villages
- Kiosk (Soochna Kuteer)
- Cities
- Blocks
- Departments
- Organizations
- Agencies and Authorities
- NGOs
- Assemblies
- Interest Groups

7.2.6 Communication

Network Protocols	TCP/IP V4
Middleware Protocols	RMI-IIOP for communicating servers based on J2EE
	SOAP V1.1 for communicating with servers not based on J2EE. It can also be used for communicating with servers based on J2EE. SOAP can be used to exchange structured data as XML objects between applications or application components via an Internet protocol (e.g. via HTTP).
	WSDL 1.1 should be used for service definition purposes.
	XML Schema Definition (XSD) v1.0 must be used to specify data elements that are to be transmitted via XML schema.
Client to Server Communication	Web Services must be used for access by client applications. Web service layer enables client systems to invoke functions of that application via Http

Directory Services	LDAP v3
	UDDI V 1.0 for publishing, structured management and offering web services.
	DSML V2 is used to provide directory service as XML documents. It is especially useful in scenarios where a client (mobile device) needs to access directory information and it does not contain LDAP client.
Application Protocols	FTP for shared use of files and offers users standardized user interfaces for different file system types.
	Http is used for communication between client and web server
	SMTP/MIME-Email protocol.
	POP3/IMAP to offer electronic mailbox facility.

8. Standards for Content Management

Processes Involved

Following processes must be followed before publishing content on portal.

- Identification and preparation of Web-Content
- Submission of web content to portal administrator for publishing
- Review & approval by portal administrator before publishing

When to User Web Publishing

Public information is to be published first on the Web except where it is decided that information will not be published on the Web for reasons of:

- high cost relative to the benefit of electronic accessibility;
- low usage;
- high publication complexity; or
- low suitability for web delivery

Discovery of non-web content

Details of public information not published on the Web must be able to be discovered on the Web. A brief summary must be provided together with details on how to access a copy via email, telephone or mail.

Legal Requirements

Web publishing must comply with all legal requirements

Equity of access and maximum usability

Web publishing must ensure access to, and usability by, the widest possible target community appropriate to the service or information resource

Quality and functionality

Publishers are responsible for the content of their electronic publishing and must ensure that the services and information provided via the online environment are comparable in quality and functionality to those delivered by other means

8.1 Content Accessibility

W3C Accessibility Guidelines

All pages of all web sites must be at least Priority 1 compliant with W3C Web Content Accessibility Guidelines 1.0. Available at: http://www.w3.org/tr/wai-webcontent

Publishing Formats

Document formats which are not native to web browsers, such as Rich Text Format, MS Word, Adobe PDF and compressed archive files (e.g. ZIP), may only be used:

- when targeting specific audiences with an installed software base or realistic technical capability to use it and
- when accompanied by a summary and details on how to obtain a copy by other means, or
- when accompanied by a version in a format native to web browsers (e.g. HTML).

End User Browser Capability

Web site design, navigation and content must be functional on Internet Explorer 6 and if possible on any other browsers with significant market penetration.

Screen Resolution

Web sites must be viewable at 800x 600 pixels and in general should be scalable for use by different screen sizes and resolutions.

Printability

All pages and files must be print-friendly or have a print-friendly version.

8.2 Discoverability

Publishing

Except where this is impractical because of high cost, low usage, high publication complexity or low suitability for Web delivery, publishers must publish on the Web all the information they make public. This includes but is not limited to:

- directory information covering contact details and services;
- annual reports, strategic plans and other public accountability publications;· media releases;
- official speeches and other public information released by Ministers, holders of statutory offices or senior agency officers;
- information that will enable the public and organizations to understand the services delivered by the agency;
- information that will enable the public and organizations to understand their own obligations and responsibilities;
- information about agency powers affecting the public;· forms for public use;
- all publications released in printed or other formats; and
- information on how to access via email, telephone, facsimile or mail

8.3 Information Management

Record keeping and disposal

Organizations must create and maintain sufficient records to meet accountability and evidence obligations. This requirement would generally be met by the maintenance of a log of all changes to the web site and web pages, so that organizations are able to verify what content or transactional services were accessible from their web sites at any particular time. The disposal of web sites, web pages and supporting records must be authorized by a person appointed by state government.

Protection from unauthorized change

Web publishing and the processes that support it must comply with the Security Policy and Guidelines for authorization.

Publication status

All downloadable publications must include date and version information.

Use of copyright information

Agencies must obtain permission from the relevant copyright owner before reproducing or communicating on a web site any material, which has not been created by them.

Privacy

Web publishing and the agency processes that support it must comply with the [2]Government Information Privacy Principles.

[2] Privacy policy needs to be formulated.

9. Standards for Web Designing

9.1 Web Page Design Guidelines

- It must be ensured that user interface is **intuitive** in nature as an intuitive user interface is easy to learn.
  - Static text (labels, captions) on the screen must conform to the terminology of the business that the application supports
  - Static text (labels, captions) on the screen must follow consistent naming convention, that is same label must convey same meaning at all the places.
  - Static text (labels, captions) on the screen must be concise, convincing, and unambiguous
  - Use of icons, controls for HTML forms for different purposes like accepting text input, displaying lists, displaying calendars etc. should be consistent across the web site. That is same icon will always mean the same thing, and conversely the same thing should always be represented by the same icon.
- To ensure **non-redundancy** hence minimal user interaction, user must not be asked to provide the inputs that are available in the system in any format. It must be ensured that GUI is not redundant by requesting minimum data for an operation. For example, once data of the list of districts is entered into software's database, the user would only be asked to pick values for the district and will never be asked to enter the name of the district again at any screen.
- In order to have a consistent **navigation scheme**, system must enable user to access information or perform tasks in same manner and conditions under similar conditions.
- To prevent poor navigation **anchoring** and **signposts** must be used, making the system user-friendlier. There must be permanent objects as unchanging reference points around which the users can navigate. In case a user is lost or disoriented, she/he should be able to quickly find the permanent objects to start over again. In addition, a user's current location will be displayed in the designated area of the application so that user can track him/her self. An application must incorporate following features at minimal.
  - Link to the *"Home Page"* must be present on all pages.
  - User's current location and the navigation path that user followed must be displayed, with hyperlinks on each sub-path, on the screen.
- User interface must be **simple**. This makes system easy to use. The user should be shown only those things that she or he is supposed to see in order to accomplish a task. Special care will be taken in making sure that the user carries out the least number of interactions with application in order to execute a particular function. A pitfall that would be avoided is "featurisms," providing many features that do not add value to the user interface. Features will not be included on a user interface unless there is a compelling need for them and they add significant value to the application.
- Design must **prevent** the user from doing something that she/he is not supposed to do. This makes the system more desirable and easy to use. Users will be prevented from performing inappropriate tasks. This will be accomplished by not displaying certain elements under certain conditions.
- **Aesthetics** helps in increasing user productivity and the first impression of the web site. The user interface should be aesthetically pleasing. While aesthetics do not directly impact the effectiveness of a user interface, users will be happier and therefore more productive if they are presented with an attractive user interface. Special care should be taken with

spacing, placement of information, alignment, colours etc. to ensure an aesthetically pleasing application.

- Display data and information in a format that does not require conversion by the user and is localized to a region.
- Do not use unsolicited graphics and windows “pop-up” to the user.
- Wherever there is a need to print a document, a printer friendly version of the HTML page should be provided. This version of the page it must be made sure that when printed in grey style, all headings and text is clear and readable.
- Whenever a user leaves the website, the user must be given a feedback clearly telling that the user is moving out of the website.

9.2 Home Page Design

- Home page must use a picture/logo that follows the theme for which a web site is being developed.
- Home page must have following links
  - About Us
  - Business tag line that communicates the purpose of web site.
  - Contact Us
  - Disclaimer
  - Feedback
  - Login
  - Logout
  - Site Index
  - Site Map
- Access to home page must be enabled in all 2nd and 3rd level pages of web site.
- New changes to web site must be communicated through home page.
- Home page must introduce a user with all the topics on which a web site provides services. Prose text for introducing a topic should not be more than 25 words.
- Best efforts should be made to cover home page content in a non-scrollable view for screen resolution 800 x 600. In case a scrollable view in inevitable, priority and interesting content should be placed on top. For screen resolution 800 x 600 page dimensions 780 x 480 fits in a non-scrollable window.

9.3 Page Layout Design

- Page layout design must give web site a distinctive identity.
- Include brand logo in each and every page of the web site.
- There are various sections in a web page. Most prominent areas that deliver actual information are content display area and menus/navigation facilities. Other important sections in a web page are areas like standard links (Home, Contact Us, Feedback etc.), search bar etc, which give web page a distinctive identity. Their positions remain unchanged in entire web site. All such sections should be clearly identified and there arrangement on web page should be done in accordance to the intended audience of the web site. Each web page must have at least following section.
  - Sections to show standard link. (preferable one at top and one at end)

  - A section to show user current location. This section should be in the top portion of a web page (not necessarily top most section) so that as soon as a page is opened user gets to know about her/his current location.
  - A section to display brand logo and business tag line.
  - A section to display search bar
  - One or more sections for displaying menu.
  - One or more sections to display actual content.
- Design must follow distinct and unambiguous style for start and end of the web page. Using font style that is different from rest of the sections in a page or creating a stripe at start and end of the page one can achieve this.
- Position (either absolute or relative) of all the section in a web page must remain fixed.
- Line lengths affect reading speed and comfort of user. Studies have shown user reads faster if line length is limited to 5.5 inches to 6.5 inches. Line length for prose in a web site should not be wider than 6.5 inches and lesser than 5.5 inches.
- Text alignment must follow following standards
  - Titles: Centre Aligned
  - Headings: Left Aligned
  - Prose/Paragraph: Left Alignment
  - Table Header: If table borders are displayed then centre aligned otherwise left aligned for text column and right aligned for numeric columns.
  - Table Data: For text data left alignment and for numeric data right alignment.

9.4 Navigation

- All web pages must provide feedback on user's location by showing users current location on each and every web page at designated place (location bar).
- All web pages must have all standard links like home page, site map, site index etc.
- All pages must give user to options for navigating back to opener. That is
  - In case of a navigation option leads to new page in new window, its control box must be enabled.
  - In case a navigation option leads to a new page in same window, user must be able to navigate back to previous page by clicking links on location bar.
- On long pages provide a table of content with links that takes users to corresponding content farther down the page.
- All tag labels on navigation links must be concise and must convey their respective functions and destinations
- Use site map so that content at any depth can be easily located
- Use site index (alphabetical listing of web page) with links to all relevant and important pages in the web site.

9.5 Scrolling and Paging

- Instead of giving long scrollable pages, prefer to use paging for different topics.
- **Rapid Scrolling:** In case if a topic is lengthy enough and paging breaks the logical grouping of sub-topics, all sub-topics must be identifiable clearly as to help user to find

sub-topic of the user's interest without having user to scan through first few lines of each and every sub-topic to make this decision.

- There must not be any horizontal scrolling for chosen screen resolution and monitor size. For Uttaranchal Portal standard for screen resolution is 800 x 600 and monitor size is 15 inches.

9.6 Heading, Titles and Labels

- Most of the user spent considerable amount of time in scanning rather than reading information in the web site. Thoughtfully designed heading, titles and labels facilitate both reading and scanning.
- At the top of the page topic should be displayed clearly about which information is being furnished. Each page should have a unique and distinctive title.
- For each category in a topic a distinctive heading is to be given. Heading can be nested however nesting of heading beyond 3 levels of depth is not recommended.
- All web pages must follow a uniform style for titles and headings so as once user is accustomed to the web site.
- Different font sizes and weights must be used for title and headings at different level of depth so that user gets the sense of hierarchy of the information in a topic.
- Highlight critical data on the screen.

9.7 Hyperlinks

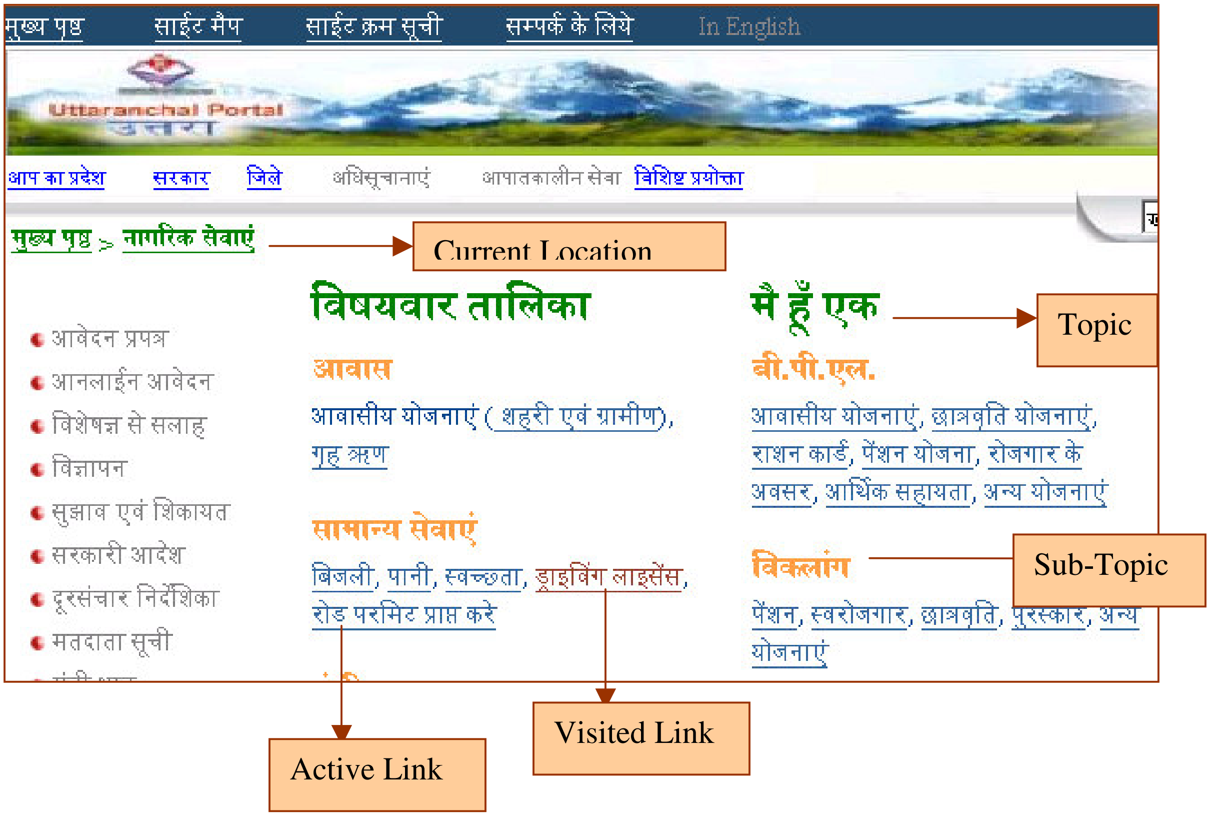
- Any hyperlink on a page must be underlined so that user knows just by viewing at text this it is a hyperlink.
- Designate visited links by changing the colour to indicate to users when a link has been visited.
- Use text links rather than image links.
- Use link labels that are easily understandable by the end users.
- Introduce redundancy and cross linkages for redundant links.
- Provide links to the related topics in each web page.
- Use appropriate line lengths for text provided for a link to remove unwanted wrapping.
- If a links takes user outside the web site, indicate that just beneath the link.
- If an image is used for navigation option, clearly mark the clickable part of the image.

9.8 Text

- Ensure visual consistency by using same style for a given purpose.
- For Hindi display in Unicode use font "Raghu" or "Devanagari MT for IBM".
- Font size should be specified in pixels. Font sizes for headings, titles, labels etc. are given in following table that ensure a proper readable display for font "Devanagari MT for IBM". (Following table intends to give an example only. It is not supposed to be followed as it is.)

Sr.No.	**Propose**	**Style Name**	**Style Specification**
1.	Body of a HTML document	BODY	**font**: 14px Devanagari MT for IBM;

Sr.No.	Propose	Style Name	Style Specification
			background-color: #FFFFFF;
2.	Active Link (unvisited and hover)	A:active, A:hover	**font-size**: 14px; **color**: #ff9900
3.	Link (visited)	A:visited	**font-size**: 14px; **color**: #954337
4.	Current Location of the user	CurrLocation	**font-size**: 14px; **color**: green
5.	Title of a information service	ServiceTopicCat	font-size: 24px; color: green
6.	Sub-topic inside a category	ServiceTopicHdr	font-size: 18px; color: #FF9C40



मुख्य पृष्ठ > नागरिक सेवाएं

विषयवार तालिका

आवास

आवासीय योजनाएं (शहरी एवं ग्रामीण), गृह ऋण

सामान्य सेवाएं

बिजली, पानी, स्वच्छता, ड्राइविंग लाइसेंस, रोड परमिट प्राप्त करे

मै हूँ एक

बी.पी.एल.

आवासीय योजनाएं, छात्रवृति योजनाएं, राशन कार्ड, पेंशन योजना, रोजगार के अवसर, आर्थिक सहायता, अन्य योजनाएं

विकलांग

पेंशन, स्वरोजगार, छात्रवृति, पुरस्कार, अन्य योजनाएं

Figure 2. Sample Picture Displaying Main Styles at resolution 800x600

- Use sufficient white spaces for uncluttered presentation.
- Change font characteristics for emphasising important characteristics for a word or phrase.

9.9 Screen based controls

- Identify required fields in a form by using a visual clue e.g. using a different colour or placing an asterisk (*) after each mandatory field label.
- Use computer to detect the errors made automatically. E.g. if a user enter her/his name in a date field, pop-up a message for this erroneous input.
- Use labels for data entry fields that are personalized and conforms to the business/user terminology.
- Put labels close to the data entry fields. There shouldn't be much gap between a label and data entry field.
- Display default values automatically to the user.
- Do not request information, which is already present in the database to minimize user interaction.

9.10 Content Organization

- Use multiple tiers in which each tier is an exploded version of information in preceding tier.
- Home page of the web site is root and must follow guidelines mentioned in Home Page Section.
- Page linked to the home page that is next tier, must introduce user to the corresponding topic and provide access to the level 2 and 3 tier pages.
- Instead of having a very deep hierarchy, emphasis should be on having a broader first level tier. Usually users do not prefer to go beyond 3rd level.
- For arranging content with in a page, high priority content should come on top followed by content in order of their priority.
- Related content in a page must be grouped together.
- Facilitate scanning of a web-page by putting well organised heading and titles.

9.11 Miscellaneous

- There must be a section called **miscellaneous** in all the pages. This section must provide information on following topics
  - Tools of web site like accessibility tools, personalization tools etc.
  - Information on supported and required plug-ins to view a site.
  - Information on fonts needed to view the site.
  - Configuration examples for browser and client PC to view the site.
  - Links for downloading certain softwares that are available free in public domain.

10. Standards for Security

Uttaranchal Portal Application will comply with the BS-7799 security requirements for System Development and Maintenance. Following is the security policy tailored for Uttaranchal portal based on BS7799 guidelines. However to be completely compliant with BS7799 or any other such specification where scope of security is not only protecting the data in electronic format but to protect the data available in any other format namely paper, humans etc, a comprehensive study is needed in identifying the security needs, security assets of the state government and formulating and implementing policies to protect those assets.

This document does not cover following points as prior to coming up with standards for a study is needed to identify assets to protect, associated risks their mitigation and contingency plan to arrive at a security policy and assets repository.

- State Security Policy
- Organizational Security
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communication and Operations Management
- Access Control and Management
- Business Continuity Management

10.1 Application Security Goals

1. Authentication: The means by which communicating entities (for example, client and server) prove to one another that they are acting on behalf of specific identities that are authorized for access.

2. Access control for resources: The means by which interactions with resources are limited to collections of users or programs for the purpose of enforcing integrity, confidentiality, or availability constraints.

3. Data integrity: The means used to prove that information has not been modified by a third party (some entity other than the source of the information). For example, a recipient of data sent over an open network must be able to detect and discard messages that were modified after they were sent.

4. Confidentiality or Data Privacy: The means used to ensure that information is made available only to users who are authorized to access it.

5. Non-repudiation: The means used to prove that a user performed some action such that the user cannot reasonably deny having done so.

6. Auditing: The means used to capture a tamper-resistant record of security related events for the purpose of being able to evaluate the effectiveness of security policies and mechanisms.

10.2 Application Security Architecture Goals

This section describes the goals for security architecture for an application.

1. Portability: The security architecture must support the “Write Once, Run Anywhere” application property.

2. Transparency: Security implementation must be transparent in behavior as it does not knows/depends the actual security implementation done by the application server provider.

3. Isolation: Authentication and access control provided is according to instructions established by the security policy makers using deployment attributes, and managed by the system administrator. Note that divorcing the application from responsibility for security ensures greater portability of applications.

4. Extensibility: The use of platform services by security aware-applications must not compromise application portability. This is achieved by restricting applications interactions to the provided APIs it will retain portability.

5. Flexibility: The security mechanisms and declarations used by an application should not limit to imposing a single security policy, but facilitate the implementation of security policies specific to the particular context and facilitate changing security policies in response to changing business needs.

6. Abstraction: This application’s security requirements will be logically specified using deployment descriptors. Deployment descriptors will specify how security roles and access requirements are to be mapped into environment specific security roles, users, and policies. A Security Administrator may choose to modify the security properties in ways consistent with the deployment environment. The deployment descriptor documents which security properties can be modified and which cannot.

7. Independence: Required security behaviors and deployment contracts should be implementable using a variety of popular security technologies.

8. Compatibility Testing: The application security requirements architecture must be expressed in a manner that allows for an unambiguous determination of whether or not an implementation is compatible.

9. Secure interoperability: Application components are able to invoke services provided in a J2EE product from a different vendor, whether with the same or a different security policy. The services may be provided by web components, enterprise beans, web services etc.

10.3 Application Security Policy

10.3.1 Authentication and Authorization

Authentication and authorization must be implemented through Common Secure Interoperability (CSI), Version 2.0, single sign-on and LDAP for User Registry. Instead of building custom authentication and authorization services, authentication and authorization services provided by application server containers must be used to make sure that security is well in place across the process boundaries of Web Container and business component container and security context is shared between all virtual machine on which application is running. This security control will be built into application.

10.3.2 Access Rights on Data

System must cater for authorization at data level. A user should be allowed to access data that belongs to the user, user's organization and user's sub organization. For example a user belonging to Jal Santhan, Nainital should be allowed to access data of Jal Sansthan, Nainital only unless there is a business requirement to access data of other organizations also. This security control will be built into application.

10.3.3 Web Based Security Policy Management

There should be a web-based tool for management of security policies like access rights, authentication information, data access policies. This control is implemented at application level.

10.3.4 Delegation of Administrative Powers

Application shall allow an administrator to delegate some of its administrative powers to other users.

10.3.5 Password Policy

Application shall allow defining a password policy e.g. password must be 8 characters long, it must contain a special character. It will help in enforcing users to use password that are harder to guess. It will also allow setting a time period after which password will get expired to make sure that user change password at regular intervals. This security control will be built into application. Recommended password policy is as follows.

Password Validity:
All system-level passwords (portal administrator, departmental administrator and other administrators) must be changed on at least a month basis.

- All user-level passwords must be changed at least every three months.
- A user can change password any time the user wants to.

Password Construction Guidelines:

- The password must be eight characters long.
- It must contain both upper case and lower case letters.
- It must contain at least one special character.
- It must contain at least one digit.

10.3.6 Self Service

System will allow defining which attributes are allowed for self-service and which attributes require approval through workflow.

10.3.7 User Account Locking

System must be able to lock a user account after a predefined number of unsuccessful logon attempts. There may be an option of automatic activation after N number of hours following deactivation or activation of account by the administrator after establishing user identity. This control will be implemented at application level.

10.3.8 Validation of Content

Application component will validate data before using that in any transaction. Also any content that is published on portal (Application form, GO, a Web Page) must undergo an approval process. This security control will be built into application.

10.3.9 Identity Management

Identification mechanism should not rely only on user login and password instead a more trusted mechanism should be used to identify a user. This will be enabled using PKI and smartcards. This security control will be built into application.

10.3.10 Server Access Log

System must maintain server access logs to find out who accessed the server. This control is implemented at application level.

10.3.11 Cookies

At client site use of cookies should be avoided and any private information should not be cached for performance reasons. One must not store sensitive information like passwords, credit card numbers etc. in cookies. After user leaves the site all cookies must be deleted to ensure that no body is able to tamper cookies. This control is implemented at application level.

10.3.12 Transmission Security

Transportation of sensitive information like credit card number etc. must be done via SSL V2.0. This control is implemented at the level of software environment setup.

10.3.13 Encryption

Any data, which is sensitive in nature, must be persisted in encrypted format so that it is not legible. Standards algorithms are DES, AES, Blowfish etc can be used to encrypt data. Preferred algorithm is 3-DES (has some performance implications). Simple DES algorithm is not recommended. This control is implemented at application level.

10.3.14 Auditing

Auditing will be performed to track malicious transaction done on sensitive data. An audit trial must include information on date of data creation, name of user who created, date of last modification and user who last modified the data. This control is implemented at application level.

10.3.15 Server Hardening

In order to ensure that unused ports of server are closed, server hardening will be done. This control is implemented at hardware/infrastructure level.

10.3.16 Terminal Authentication

System will be able to identify terminal and deny access to the terminals, which are not allowed access to the system. This control will be implemented at infrastructure level. However implementation of this policy can be deferred till we have a WAN that connects all departments and data center.

10.3.17 Terminal Logon procedures

A user cannot logon from anywhere else apart from her/his designated terminal. This will apply only to special users like departmental users, district magistrate, kiosk owner etc however to enforce this policy terminal authentication is pre-requisite.

10.3.18 User Access Right on Terminals

Unless it is required a special user should not be given administrative privileges/power user rights like installing software on her/his terminal, using which portal she/he will be accessing the portal application. Implementation of this control requires auditing.

10.3.19 Prevention against Security Threats

Following section lists some of the possible security threats and the prevention measures taken for such threats:

- SQL injection
- Buffer overflows
- Cross-site scripting

- Forceful browsing
- Cookie tampering
- Form-field manipulation
- Denial of Service and Distributed Denial of Service

10.3.20 Database Security

In order to enforce security at database level, application database structure will have following features:

- Encryption of critical/confidential data (such as user passwords, credit card information etc).
- Logging of user actions at database level to support Non Repudiation.
- Database will have IP based access definitions, so that only application server can connect to the database.

10.4 Firewall Standards

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. Basically, a firewall, working closely with a router program, filters all network packets to determine whether to forward them toward their destination. A firewall is often installed away from the rest of the network so that no incoming request can get directly at private network resources. There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain names and IP addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates.
Following are the few considerations, which we must be taken into account while deploying a firewall:

- Regular Auditing – This is required to ensure that everything is working in order.
- Logs – Proper logs are to be maintained in order to trace any problems/security breaches, which can occur during normal operations.
- Intrusion Detection- Firewall should be able to detect intrusion attempts.
- Contingency Planning – In case of failure of firewall, there should be plans to recover immediately
- Firewall Access Privileges- Access privileges should be controlled by procedures defined by the organization deploying firewall.
- Disclosure of Internal Network Information- Internal network information must be confidential, proper measures must be taken to ensure confidentiality.
- Posting Updates- If some updates/patches are released for the firewall they must be installed in acceptable time from the release date.
- Monitoring Vulnerabilities- system security should be checked at regular intervals by created false attacks on the system, in order to ensure that system is secure.
- Standard Products- standard products must be used as firewall.

10.5 Physical Security Standards

Physical security safeguards need to be considered for information resources residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (in-transit facility housing). Appropriate physical safeguards need to be established based on the risks related to geographic location, including natural threats (such as flooding), man-made threats (such as burglary or civil disorders), and threats from nearby activities (such as toxic chemical processing or electromagnetic interference). Lastly, physical safeguards need to assure that the appropriate levels of support facilities such as electric power, heating, and air-conditioning are sustainable as required by the information resources.

For example, physical access controls may be used to restrict and monitor the entry and exit of personnel to/from a room, a data center, or a building. Physical access controls may range from badges and locks to retina scanning personal identification devices and vibration detectors. Physical access controls need to be considered for those areas containing system hardware, as well as for those areas which house network wiring, electric power, backup media, source documents, etc.

Physical security safeguards provide a first line of defense for information resources against physical damage, physical theft, unauthorized disclosure of information, loss of control over system integrity, and interruption to computer services.

Standards

- Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.
- Access to "critical" computer hardware, wiring, displays and networks must be controlled by rules of least privilege.
- System configurations (i.e., hardware, wiring, displays and networks) of "critical" systems must be documented. Installations and changes to those physical configurations must be governed by a formal change management process.
- A system of monitoring and auditing physical access to "critical" computer hardware, wiring, displays and networks must be implemented (e.g. badges, cameras, access logs).
- Low and medium risk equipment should be protected by an appropriate alarm system in addition to the correct security enclosures.

10.6 Anti Virus Software Requirements at the Client PCs

Every Client PC should be with virus protection software. There will be scheduled anti-virus updates at regular intervals (For example once in a week).

Virus tools tend to have three functions:

- Generic monitoring (prevention)
- Scanning (looking for viral signatures)
- Integrity checkers (looking for changes in files)

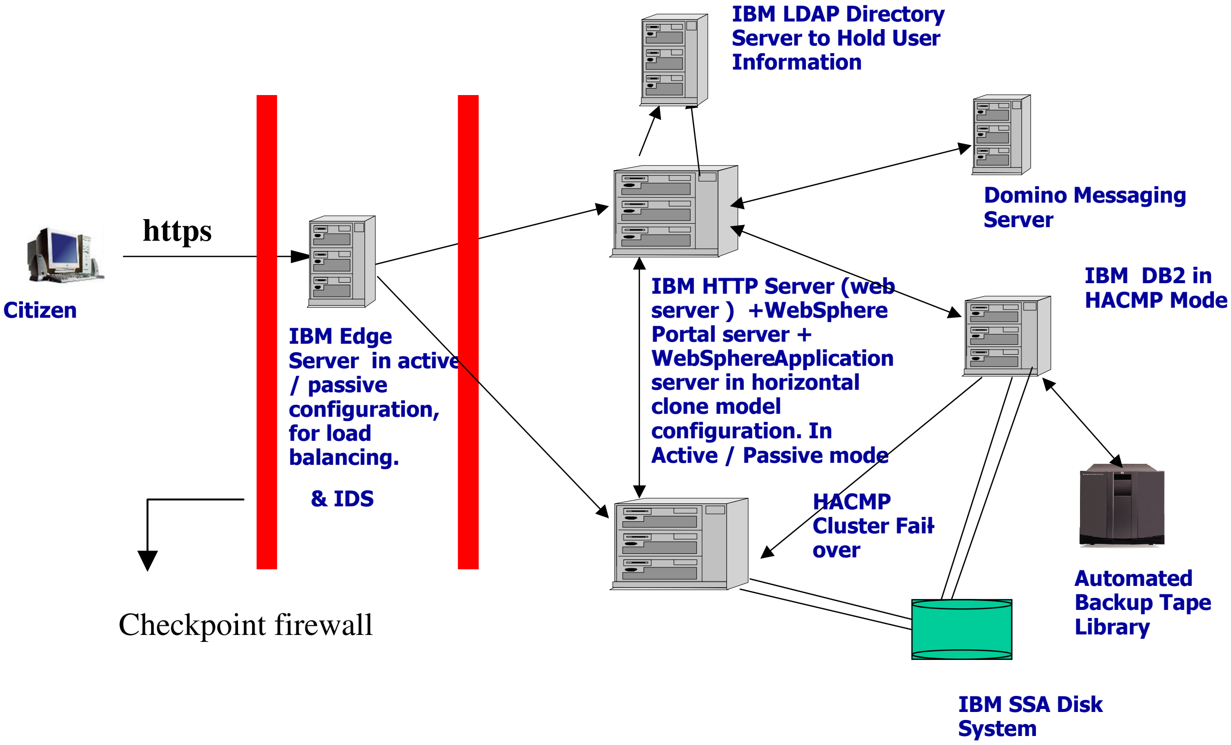
There are literally hundreds of anti-virus programs available. Typically an enterprise buys a site wide license for all machines with regular (e.g. monthly) automatic updates. Anti-virus software to be used must fulfill following criteria:

- It will work with Win95, Win 98, Win NT, Win Me, Win 2000, Win XP.
- It will protect against macro viruses (i.e. viruses in MS-Office documents or other desktop applications which may contains macros) and possible ActiveX viruses.
- Its user interface should be friendly and easy to use (minimum user education necessary).
- It will be possible to upgrade the anti-virus from a server quickly, regularly and easily.
- Some examples of current products are: McAfee, Norton Anti-virus, IBM AV (Anti-Virus).

Annexure A

1. UA Portal Architecture

Given below is the architectural diagram of Uttaranchal Portal, an end citizen (Kiosk Owner) will access the citizen portal system via browser interface. The request will first go to the IBM edge server first. The edge server is the component, which can work as reverse proxy or load balancer for the web server.


IBM LDAP Directory Server to Hold User Information
Domino Messaging Server
https
Citizen
IBM Edge Server in active / passive configuration, for load balancing.
& IDS
IBM HTTP Server (web server) +WebSphere Portal server + WebSphereApplication server in horizontal clone model configuration. In Active / Passive mode
IBM DB2 in HACMP Mode
HACMP Cluster Fail over
Automated Backup Tape Library
Checkpoint firewall
IBM SSA Disk System

Deployment View for Portal in Clustered Environment

The edge server will be responsible to forward the request to the active IBM HTTP web server. The IBM HTTP web Server will be configured in active / passive mode to ensure the high availability of the solution. Initially the edge server will be configured to forward the request to the primary (active) web server and primary web server will be responsible to forward the request to the WebSphere Portal Server. In case the primary web server is not available, the request from edge server will be forwarded to the secondary web server, which will act as active web server in the event when primary is not available.

The information about the citizen or register users will be stored in LDAP based IBM directory server. The IBM directory server is LDAP based directory server which come bundled with WebSphere Portal server and is used store the authentication and authorization information about the user of the citizen Portal hosted on to the WebSphere Portal server. Different Authorization rules like giving access to different information, data, application based on the role of user can be defined by the administrator of the centralize system using administrative module of the WebSphere portal server. To ensure the high availability of the LDAP server / user information the IBM LDAP server will be installed in master / slave relationship configuration.

WebSphere Portal server will be used to host centralize application which will contain the different information / application like Government and ministry related information, recent press release, latest news about the Government, citizen guide, Government forms and format etc. The various applications, which will be hosted on the portal, will be developed using JAVA, JSPs, Servlets, EJBs and Web Services. These applications will be developed using WebSphere Application development environment (WSAD), which is an integrated development tool by IBM and can be hosted onto the WebSphere Portal server. The WebSphere Portal server will also be installed in the clone model where exact replica of the application will be running at the multiple places so that in the event one instance of the application is not available the other instance can be used to server the request.

DB2 will be used to hold the transactional data and other related data. To ensure the high availability of the data, the DB2 database will be installed in highly available cluster environment.

Domino messaging server will be used as mail server. The access to the mail server will be given via Portal framework by using iNotes portlet. The iNotes portlet comes bundled with the WebSphere Portal server and is used to give access to the mail via browser-based interface in the portal server environment.

The portlet API is an extension of the servlet API, except that it restricts certain functions to a subset that makes sense for portlets running in the context of a portal. For example, unlike servlets, portlets may not send errors or redirects as a response. This is only be done by the portal itself, which controls the overall response page. Usually, many portlets are invoked in the course of handling a single request, each one appending its content into the overall page. Some portlets can be rendered in parallel, so that the portal server assembles all the markup fragments when all the portlets finish or time out. Portlets that are not considered thread-safe will be rendered sequentially. The latter is in accordance with J2EE specifications.

To implement PKI, certificates will be installed on the web server and client machines. Https protocol will be used for PKI enabled system.

Smart card integration requires a smart card, smart card reader and writer. Smart card readers are able to invoke web services that are running on the application server. That means any functionality that is exposed as a web-service can be driven by a smart card. For example user authentication program will be implemented as a web service. To login into the system using smart card one has to swipe card in smart card reader and then reader invokes the authentication web-service and passes user's credentials to the web-service. This web-service uses information passed by smart card for authentication and then logging the user in.

Antivirus software will be installed on all the machines and servers.

Firewall to be used in Uttaranchal Portal System will be Checkpoint Firewall in conjunction with RealSecure Network Sensor.